IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

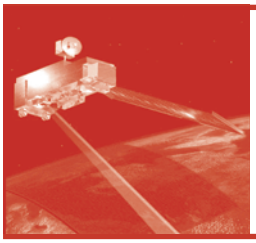
OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION

16 janvier 2013

Faux, rumeurs et désinformation dans le cyberespace

SOUS LA DIRECTION
DE FRANÇOIS-BERNARD HUYGHE

DIRECTEUR DE RECHERCHE A L'IRIS



Internet ou la vérité de l'illusion

Que cachent nos écrans ? Il ne se passe pas de jours où la question du vrai ou du faux sur Internet, du trucage ou de la mystification, de la désinformation et de la rumeur ne se trouve au premier plan de l'actualité. Le jour où nous écrivons, nous apprenons qu'un article de l'encyclopédie en ligne Wikipedia présentait une guerre purement imaginaire en Inde ou que sur Twitter a été annoncée une fausse mort de l'auteur de la saga Harry Potter. On signale également de pseudo messages de gendarmes et des usurpations d'identité. De même, un quotidien présente une étude des diverses escroqueries à la carte de payement qui reposent notamment sur la fabrication de faux sites bancaires. Le faux semble être partout !

Et, du reste, les autorités politiques ne cessent de se heurter à la difficulté de savoir qui a vraiment émis tel message et qui menace réellement la sécurité informatique ou l'ordre public. Ainsi, la Chine impose l'obligation d'enregistrer leur véritable identité à tous ceux qui s'expriment en ligne. En France, une ministre réclame à Twitter un dispositif qui favorise les dénonciations directes de propos scandaleux (antisémites ou homophobes) et l'identification de leurs auteurs (qui se trouveront sans doute être dans de nombreux cas des gamins troublés par la puberté).

Le faux – fausses nouvelles, faux partisans, faux interlocuteurs, fausses images – est contagieux. Qui vous garantit que votre interlocuteur en ligne n'est pas un faussaire, voire un algorithme créé pour produire artificiellement des mouvements d'opinion ? Olivier Kempf s'interroge sur cette identité réelle ou numérique, source de tant d'inquiétudes. Frank Bulinge décrit les mécanismes qui font d'Internet un formidable accélérateur de rumeur, mais aussi sur nos faiblesses qui font que nous sommes si réceptifs à de telles tromperies. Laurent Gaildraud, pour sa part, étudie les facteurs qui font le succès ou l'échec de la rumeur, en particulier électronique, voire sur les stratégies que l'on développe pour s'en protéger. Maxime Pinard nous rappelle que le réseau est aussi à l'origine de comportements et de techniques de vérification, qu'elle soit citoyenne ou médiatique

Enfin, nous concluons en analysant le rapport entre la technique numérique ou la structure des réseaux et cette exceptionnelle faculté de rendre le faux contagieux, mais aussi de faciliter les procédures de vérification. ■

François-Bernard Huyghe

Être, paraître et usurper dans le cyberespace

Entretien avec Olivier Kempf
Maître de conférence à l'Institut d'Etudes Politiques de Paris,
Auteur de* Introduction à la cyberstratégie, *Ed. Economica, 2012
Propos recueillis pas Pierre-Yves Castagnac

IRIS : Avant d'explorer la question du faux, qu'est-ce que l'identité réelle d'un individu ?

Olivier Kempf : Sur le plan administratif, l'identité d'un individu est avant tout représentée par sa carte nationale d'identité. Il s'agit d'un document officiel qui mentionne quelques caractéristiques : nom, prénom, date de naissance, taille, etc. Mais derrière cette identité publique, il existe une identité intime qui est plus riche et plus complexe. Elle dépend d'un vécu mais également de références familiales, amicales, scolaires et professionnelles. On peut être né d'un père alsacien et d'une mère bretonne. On peut être né à Marseille mais vivre à Paris. On peut se sentir Français tout en étant Européen. L'individu est ainsi composite. Ce « tout » est cependant parfaitement fonctionnel. Au fond, dans cette question de l'identité, il est nécessaire de se demander : qu'est-ce qui fait que l'on est « soi » ? Quelles sont nos références dans la vie de tous les jours ?

IRIS : De quelle manière retrouve-t-on cette complexité dans le cyberespace ?

Olivier Kempf : Si dans la vie réelle, la notion de l'identité intime est complexe, il en va de même dans le cyberespace. L'individu n'en a d'ailleurs pas forcément conscience… mais, il a, nécessairement plusieurs identités. Par « identité », il faut comprendre « code », « référence ». L'individu est identifié par des chiffres, des lettres. Il s'agit d'identifiants qui lui sont propres. Ils lui ont été attribués par un opérateur. Ce qui permet à ce dernier de l'identifier directement. On peut parler de « référence client ». Chaque site a les siennes. Les numéros que l'on vous demande sont, à chaque fois, différents, mais l'on s'aperçoit que le seul dénominateur commun, c'est « vous ».

IRIS : Il s'agit là du volet technique de l'identité… mais il est également possible de se créer des pseudos.

Olivier Kempf : Exactement ! Ces « codes » que je viens d'évoquer concernent un aspect technique. Un opérateur vous impose un identifiant. Cependant, un individu peut également se créer ses propres identifiants : adresses mails, pseudos, avatars… Il peut ainsi exister sous plusieurs noms. Un individu peut ainsi avoir plusieurs adresses mails. Elles peuvent êtres imposées car il a plusieurs fournisseurs d'accès (@yahoo.fr, @gmail.com, @hotmail.fr…), mais il peut également se créer son propre carnet d'adresses personnel. Il va séparer l'adresse mail professionnelle de celle pour ses amis ou encore pour sa famille. Un individu est ainsi pluriel dans le cyberespace. Certaines adresses peuvent être proches de mon être social. D'autres, au contraire, sont plus éloignées… Nous pouvons encore complexifier cette notion d'identité en évoquant les pseudos et les avatars. L'individu peut se cacher derrière un nom d'emprunt. Une personne s'appelant dans la vie réelle « Jacques Martin » peut se faire appeler « John Smith » ou encore « Gandalf ». Internet favorise l'usage des pseudonymes. Les réseaux sociaux et les plateformes de discussions permettent de multiplier les noms d'emprunt. Tous ces pseudos ou avatars sont l'expression de notre identité. Mais comment rapprocher « Gandalf » de « Jacques Martin » alors que l'on est extérieur au cercle intime ?

IRIS : A partir de quand passe-t-on dans l'illégalité ?

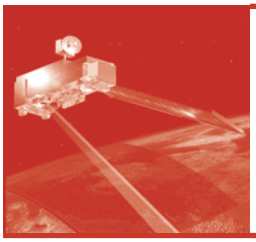
Olivier Kempf : L'illégalité commence avec l'usurpation d'identité. S'il est possible de se créer des pseudos, il est également possible d'usurper l'identité d'un individu. Autrement dit, quelqu'un peut se faire passer pour soi dans le cyberespace. Il a donc la capacité de voler une part de mon identité. Dans la vie réelle, c'est exactement la même chose : si je perds ma carte d'identité ou mon passeport, quelqu'un peut s'en servir et voyager avec. Sur internet, les procédures de falsification sont cependant rendues plus faciles. Le réel souci vient surtout de la vérification de l'identité : comment prouver qu'il s'agit bien de moi ? Si « Jérôme Durant » décide de s'appeler « Jacques Martin » sur Internet, il en a le droit. Internet est un espace libre. Jusqu'à présent, c'est moi qui donnait de la cohérence à mes identités, Mais subitement, quelqu'un peut prétendre être moi à ma place. Que faire si « Jérôme Durant » commet des actes répréhensibles au travers de son alias « Jacques Martin » ? Le vrai « Jacques Martin » va avoir du mal à prouver que l'alias ne lui appartient pas. Internet est un espace de liberté, mais il pose le problème de la maîtrise de cette liberté. Il n'est pas possible de contrôler totalement cet espace.

IRIS : Existe-il des moyens de combattre cette usurpation d'identité ?

Olivier Kempf : Il existe, d'un côté, une action de l'individu et, de l'autre, un environnement dans le cyber. D'où les questions : que peut-on faire sur l'individu ? Et que peut-on faire sur le cyber ? L'individu doit d'une certaine façon maîtriser sa propre liberté et essayer de la contrôler. Il doit être prudent : ouvrir, par exemple, un compte sur chacun des grands réseaux sociaux (Twitter, Facebook…) et y avoir une présence minimale. Dans un deuxième temps, il peut encourager les associations de consommateurs pour s'adresser aux opérateurs. Il existe donc une action individuelle de prévention et une action collective de soutien. Derrière le consommateur, il y a le citoyen. Sur une autre échelle, l'individu va devoir faire confiance à ce qu'on appelle l'ordre public… autrement dit, à l'Etat. Un Etat peut émettre des règles de droits pour tous ceux qui vont pratiquer le cyberespace sur son territoire. Les Etats possèdent, en effet, les outils de la violence légitime avant de parler des gendarmes. Il s'agit de l'édiction du droit, et de son respect par la justice. Avec en permanence à tenir la balance égale entre la nécessaire protection des citoyens et le respect indispensable des libertés individuelles.

IRIS : Une dernière question, qu'en est-il des robots (bots, spy bots, DDOS…) ?

Olivier Kempf : Ils constituent un autre aspect de l'usurpation d'identité : à ceci prêt qu'on ne cherche pas à attaquer l'identité de l'individu, mais juste à l'utiliser pour se camoufler. En effet, la procédure consiste à installer un petit logiciel furtif qui utilisera votre ordinateur sans que vous en ayez conscience. Du coup, cet ordinateur servira de relais pour participer à des attaques collectives. C'est le mécanisme sous-jacent aux attaques dites DDOS (déni de service distribué) qui utilisent des masses d'ordinateurs « zombies » pour lancer des requêtes contre un serveur ciblé. Au fond, votre « identité » est empruntée, sans grand dommage pour vous puisque la masse dissout votre participation relative. Il y a donc un double processus d'anonymat : celui d'un individu perdu dans une masse d'attaques, et celui de l'ordinateur qui sert d'écran au vrai manipulateur qui orchestre l'opération. Voici encore une illustration de la complexité de l'identité sur le cyberespace, qui mériterait un livre entier ! ■



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

iRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Internet est-il un accélérateur de rumeur ?

par Franck Bulinge,
Maître de conférence, Professeur à l'Institut supérieur de commerce de Paris
Docteur en Sciences de l'information et de la communication

Par l'intermédiaire du courrier électronique, des listes de diffusions et du web, Internet permet de véhiculer une quantité vertigineuse d'informations. Cette surabondance d'information pose le problème du choix, mais également du discernement et de la capacité de traitement. C'est sans doute à cause de cette infinité de choix que l'on pourrait percevoir a priori Internet comme un « accélérateur » de rumeur. On constate de fait un fort développement des « rumeurs électroniques », selon Emmanuel Taïeb qui souligne au passage l'identité de nature entre la rumeur et Internet. L'une comme l'autre obéissant à une « nécessité de circulation », Internet apparaît dès lors comme le véhicule idéal pour la diffusion des rumeurs. Pour Pascal Froissart, « parce qu'Internet propose une orgie de textes dans tous les genres, parce que le réseau des réseaux semble gouverné par tout le monde ou personne, parce que n'importe qui se connecte à n'importe quoi, parce qu'aussi Internet est une mécanique complexe, on a pu dire qu'Internet était le médium rêvé de la rumeur »

Le réseau mondial, ou Web, à travers les sites, blogs, Wiki, forums, listes, chats, permet d'émettre des hypothèses, des théories qui peuvent être présentées, perçues ou interprétées comme des certitudes. « Toute personne qui a une théorie possède maintenant un mégaphone » titrait le journal USA Today. Il est intéressant de noter que toutes les situations angoissantes ou de tensions mondiales peuvent susciter une vague de fantasmes sur Internet, lesquels se nourrissent et alimentent la théorie du complot. En ce sens, Internet ne fait qu'amplifier des états socio-psychologiques provoqués par les crises, lesquelles se caractérisent par une augmentation de l'état d'incertitude et des facteurs anxiogènes, très fertiles en termes de rumeur.

Medias Internet versus medias de presse ?

L'idée qu'Internet est un réseau anarchique où circule des informations douteuses est communément répandue. Internet, identifié comme l'espace de toutes les dérives et de tous les dangers, est rapidement montré du doigt jusqu'à devenir l'emblème spectral de la manipulation des masses. Ainsi Internet favoriserait la rumeur tandis que l'information fiable serait communiquée par d'autres médias.

Cette condamnation est-elle réellement fondée ? Ne cache-t-elle pas dans certains cas une réaction aux progrès des technologies de l'information et de la communication, face à la remise en cause possible du rôle prédominant de la presse en matière d'information ?

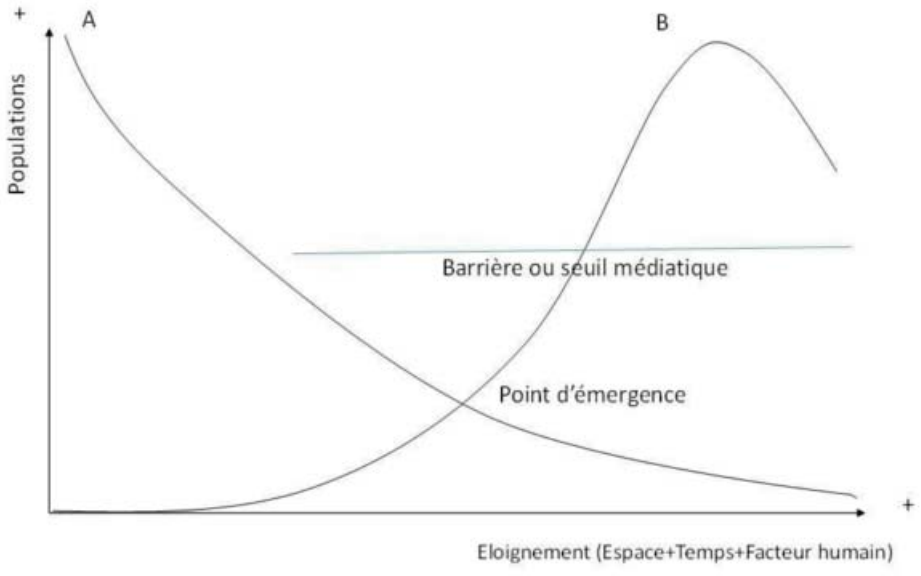
Il est certain qu'Internet offre des possibilités de trucages et de manipulation susceptibles d'engendrer la rumeur. Cependant, les autres médias, à commencer par la presse, sont-ils plus fiables ? Dans un contexte d'industrialisation de la presse, les journalistes n'apparaissent plus, aux yeux du public, comme les garants d'une information propre et fiable. L'information de presse, répondant à des critères économiques, tend à devenir uniforme. Dans certains cas, la rumeur franchit même la barrière déontologique des journalistes et se répand dans la presse. ■■■

Pascal Froissart considère que loin de se diffuser accidentellement via les medias, la rumeur « se meut via les medias d'abord et avant tout ». Cela serait d'autant plus vrai pour les rumeurs d'ordre économique qui n'ont de sens que lorsqu'elles touchent un public extrêmement ciblé (salles de marchés, actionnaires, décideurs…).

Le cycle de vie de la rumeur

Il semble qu'il existe une relation d'une part entre la fiabilité de l'information représentée par la courbe A, et le niveau de propagation de la rumeur, et d'autre part entre ce niveau de propagation et le franchissement d'un seuil médiatique au-delà duquel la presse transmet elle aussi la rumeur.

La courbe A illustre le fait que plus nous nous éloignons de la source d'information (témoin direct), plus celle-ci devient invérifiable et par conséquent peu fiable. La rumeur, dont le cycle de vie est représenté par la courbe B, germerait dans cet état de flou informationnel, au moment où l'information devenue invérifiable mais suffisamment vraisemblable devient un facteur de lien social, sous forme d'un événement informationnel soudain digne d'être repris, porté et partagé par une chaîne d'acteurs. Pour Tamotsu Shibunati la rumeur trouve son origine dans l'interrelation entre l'importance et l'ambiguïté d'un événement : « si son importance est nulle ou si l'événement n'est pas du tout ambigu, il n'y aura pas de rumeur ».



Dès lors la rumeur prend vie et forme, grandit, s'enrichit, jusqu'à atteindre un niveau de maturité et entamer une phase de déclin, sans qu'il soit possible de dire si elle meurt véritablement ou si elle couve comme le feu sous la cendre, ce que semblent confirmer les chercheurs qui observent un phénomène de récurrence. Internet, favorise à cet égard le phénomène par la mise en mémoire des rumeurs qui, une fois émises sur la toile, sont stockées et accessibles sans limite dans le temps.

Typologie des rumeurs sur Internet

Il est nécessaire, à ce stade, d'esquisser brièvement une typologie des différents types de rumeur que l'on peut rencontrer sur Internet. Si l'on se réfère à la typologie de Véronique Campion-Vincent et Jean-Bruno Renard, on peut distinguer 7 types de messages « rumoraux » : les alertes aux virus informatiques, les chaînes magiques ou superstitieuses, les chaînes de solidarité, les pétitions, les rumeurs proprement dites ou canulars, les légendes urbaines, les histoires drôles, et les photos ou dessins humoristiques. De son côté, Didier Heiderich, outre les légendes urbaines, distingue la désinformation à but commercial, l'attaque politique, l'attaque directe d'une offre commerciale, les fausses offres commerciales, la désinformation financière, la diffa-

-mation, les opérations de décrédibilisation, l'alerte panique pour semer la terreur… Les deux auteurs résument assez bien les deux facettes de la rumeur, littéraire d'un côté, et instrumentalisée de l'autre. C'est bien entendu le second qui nous intéresse dans cet article.

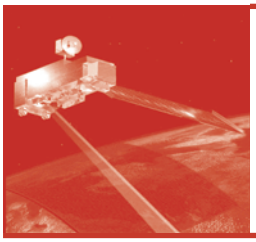
La prophétie du 11 septembre 2001

Un très bon exemple de rumeur circule depuis les attentats du 11 septembre 2001. Il s'agit de la conversion alphabétique d'une soi-disant immatriculation d'un des appareils qui a percuté le WTD. Le message invite le lecteur à convertir Q33 NY en alphabet windings sur Word. Cela donne :

Q33 NY = ✈ 🗎🗎 ☠✡

La démonstration est stupéfiante, et la plupart des individus réagissent « positivement», et transmettent le message à leurs amis. Ici les éléments de manipulation sont concentrés dans l'expression graphique et la symbolique qui s'en dégage. Dans cet exemple, on associe un fond d'antisémitisme historiquement très fertile (voir le mythe du Protocole des sages de Sion), à des affects liés au drame, l'ensemble se renforçant mutuellement au point de faire oublier la question essentielle : à aucun moment les « victimes » de ce hoax s'interrogent sur la réalité de cette immatriculation. L'esprit critique est inhibé et l'ancrage renforcé par un effet de répétition/massification dû à la propagation rumorale. Au final, il devient évident qu'un mystère plane sur le 11-Septembre, mais ce mystère est en réalité une construction collective, un mythe qui s'inscrit désormais dans la mémoire de l'humanité, et deviendra régulièrement le lieu d'émergence de nouvelles rumeurs. ■

*
* * *
*



Rumeur, mode d'emploi

Entretien avec Laurent Gaildraud,
Consultant & conférencier sur la manipulation de la rumeur,
Auteur de* Orchestrer la rumeur, *Ed. Eyrolles
Propos recueillis par Pierre-Yves Castagnac

IRIS : Au fond, qu'est-ce qu'une rumeur ?

Laurent Gaildraud : Une rumeur est avant tout un bruit informel. Il existe, il persiste, il s'évapore. Il repart aussi vite qu'il est arrivé. Il s'agit d'une, ou de plusieurs informations qui circulent et qui sont transmises par un vecteur (individus, internet…). Il n'y a pas forcement de source déterminée. On est dans le « il parait que ». Ce flou trouve sa source dans l'imaginaire collectif. Au fond, pour qu'une rumeur prenne corps, il est nécessaire de se demander : « qu'est ce que mes contemporains ont envie entendre ? ». Ces rumeurs ont certes des fonctions récurrentes mais il faut arrêter de penser que toutes les rumeurs sont orchestrées.

IRIS : Quelles sont ces fonctions récurrentes ?

Laurent Gaildraud : La rumeur est nécessairement officieuse. A partir du moment où elle devient officielle, elle perd son caractère de rumeur pour devenir information, indépendamment du fait qu'elle soit vraie ou fausse. Une rumeur a également pour vocation de contrôler les individus dominants. Tout individu important peut être déstabilisé par une rumeur. Il faut cependant garder à l'esprit que la durée de vie d'une rumeur est limitée dans le temps. Plus dans le temps que dans l'espace. Elle est généralement courte, de quinze jours à un mois. Il existe un pic gaussien à quinze jours. C'est une moyenne. La rumeur base également son résonnement sur des faits réels mais déforme cette réalité. On retrouve ainsi dans le schéma des rumeurs, des fausses informations, des canulars, des légendes urbaines… ainsi que des préjugés. N'oublions pas qu'à partir du moment où tout le monde croit en quelque chose, cette chose devient vraie. Elle s'autovalide. Enfin, une rumeur doit être quelque chose de simple et direct. Elle doit être comprise par le plus grand nombre. La simplicité la rend aisément appropriable.

IRIS : Quels sont les ingrédients d'une « bonne » rumeur ?

Laurent Gaildraud : Pour qu'une rumeur fonctionne, il est nécessaire de faire appel aux « sentiments premiers » : le rire, la joie, le dégoût, la peur… Pourquoi ces sentiments ? Car ces sentiments sont des sentiments qui sont reconnus par toutes les cultures, même celles qui sont orales. Ils font appel à ce qui est au plus profond de nous. La rumeur doit vous faire réagir. Sur un autre plan, une « bonne rumeur » doit absolument avoir une assise sociale et non pas physique. Une rumeur qui affirme que X ou Y est décédé peut être balayé rapidement : il suffit que la personne supposée morte parle pour que la rumeur s'autodétruise. En revanche, si l'on se base sur la croyance, il est beaucoup plus dur de démontrer que la rumeur est fausse. La croyance a une forte valeur sociale. Bien souvent les gens préfèrent modifier la réalité que modifier leurs croyances. En plus de faire appel aux sentiments premiers, il faut que l'auditoire soit « tendu », c'est-à-dire qu'il soit dans un contexte d'appréhension ponctuel ou à défaut, d'éveil quelconque. Prenons un exemple : une rumeur de rachat signifiant implicitement que 40% des salariés seront

licenciés. On parle alors de mise sous tension des capteurs.

IRIS : Comment lancer une rumeur ?

Laurent Gaildraud : Tout dépendra du produit… Il existe cependant certaines règles comme celle du moment. Si vous avez le choix, il est préférable de la lancer durant une période de crise : toute forme d'instabilité sociale est génératrice d'inquiétude. Et tout ce qui est anxiogène est bon pour les rumeurs car il a un besoin informationnel. De même, les anxieux ont besoin de communiquer, de se retrouver dans des réseaux sociaux… Ce besoin de communiquer propage (in)volontairement la rumeur. Facebook, Twitter, Internet vont alors servir de mégaphone. Mais la qualité de votre rumeur est infiniment plus importante que les canaux de diffusion que vous choisirez pour la propager. On peut dire sans risque que plus la rumeur sera de qualité et moins vous aurez d'efforts à fournir pour la diffuser.

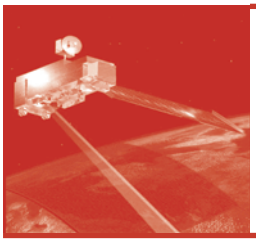
IRIS : Peut-on contrôler une rumeur ?

Laurent Gaildraud : On ne contrôle pas une rumeur. On peut l'initier, mais certainement pas la contrôler. Elle se propage d'elle-même si elle a été bien construite. Elle se diffuse et s'autoalimente des vecteurs qu'elle va croiser… un peu comme une maladie. Des mathématiciens des sciences sociales se sont d'ailleurs penchés sur le sujet. Ils ont été obligés de reprendre ce que les épistémologistes avaient fait car les modèles de propagations sont similaires. Le cercle s'élargit progressivement. La rumeur s'accroche ou non sur un individu qui devient lui-même source de diffusion. Au fur et à mesure qu'elle se diffuse, la rumeur peut muter. Nous avons déjà vu certaines catégories de rumeur se déplacer sur toute la planète. Elle subit dans ce cas des mutations culturelles. Mais s'il n'est pas possible de la contrôler, il est éventuellement concevable de booster une rumeur dans son premier demi-cycle de vie… C'est compliqué, mais faisable !

IRIS : A défaut de la contrôler, peut-on imaginer limiter la diffusion d'une rumeur ?

Laurent Gaildraud : Limiter, c'est dans un sens contrôler. Alors, sans rhétorique, il est possible, dans une certaine limite, de répondre à une rumeur. Première idée : ridiculiser la rumeur marche assez bien. Prenons l'exemple du cancer de François Mitterrand. Un journaliste lui avait posé la question et le Président de la République lui avait répondu avec un sourire : « Oui, il m'arrive d'éternuer ! ». Qui rigolerait de son cancer ? De même, deuxième idée : amener une rumeur dans l'absurde. Ce qui était jusque là probable, possible… devient alors impossible. « Non, je n'ai pas volé 50.000 euros, mais 50 milliards ! ». Troisième idée : le démenti… Un art difficile dans le cadre des rumeurs. Il ne faut pas baser son démenti sur une quelconque logique scientifique mais sur l'imaginaire. Seul un imaginaire peut répondre correctement à un imaginaire. N'oublions pas qu'il est également impossible de démentir sans propager. Il faut de la finesse et de l'entrainement pour démentir une rumeur sans en parler. En conclusion, comprendre les rumeurs, c'est aussi les appréhender. On nous répète depuis la nuit des temps que la rumeur, c'est mal ! Je pense que l'on rivalise mieux quelque chose que l'on comprend.

*
* * *
*



La vérification sur Internet : une mission sans fin

par Maxime Pinard,
Adjoint des formations à l'IRIS SUP'
Chercheur en géopolitique du cyberespace à l'IRIS

L'une des critiques majeures adressée à Internet porte sur la véracité des informations que l'on peut y trouver. De par sa facilité d'utilisation, son déploiement à l'échelle internationale, et surtout les millions de personnes qui ont rédigé tel ou tel document, on pourrait presque dire qu'Internet « regorge » d'informations. Pour être plus précis, l'inflation d'informations par rapport à la période pré-Internet n'est pas aussi flagrante qu'on ne l'imagine ; il est davantage question d'un phénomène de duplication de l'information. La conséquence première est facilement imaginable : une fausse information postée sur un blog en France peut en quelques heures être reprise par des médias étrangers en Asie ; il suffit de créer le « lien » qui médiatisera la fausse information via l'envoi à des tiers du lien vers le blog, via des tweets par exemple, jusqu'à ce que tel journaliste s'approprie l'information pour la diffuser plus largement.

Les cas de fausses informations reprises par les médias sont légion. Cela peut concerner le texte, avec par exemple une usurpation d'identité d'un compte tweeter d'une personne importante (ministre, star de cinéma…) faisant faire à cette dernière une fausse déclaration. Il peut également s'agir d'images retouchées à l'ordinateur via des logiciels spécifiques qui peuvent berner certaines rédactions qui ne se rendent compte de leur bévue qu'une fois leur numéro édité. Enfin, il y a évidemment le problème des vidéos : pour un prix modique, n'importe qui peut s'improviser journaliste, polémiste, enquêteur et réaliser des montages vidéo à même de servir ses opinions.

Le citoyen est avide d'information

L'importance de cette « médiasphère de l'information » est d'autant plus puissante qu'elle fait écho à un nouveau réflexe analysé avec précision par Raffaele Simone dans son ouvrage « Pris dans la Toile, l'esprit aux temps du web » (le Débat, Gallimard, 2012), à savoir la recherche d'informations par le citoyen sur Internet, soit comme source directe, soit comme source complémentaire des médias dits traditionnels. Il est d'ailleurs fort probable que les générations actuelles et futures auront tendance à privilégier l'information numérique, ne serait-ce que par l'explosion des terminaux d'accès à Internet qui en facilitent grandement la consultation.

Ce succès de l'information en ligne ne doit pas cependant laisser croire que les cybernautes donnent carte blanche aux sites qu'ils consultent. L'actualité est émaillée d'histoires plus ou moins graves, où une fausse information a été repérée, soit rapidement, soit parfois après plusieurs années d'existence. Wikipedia est souvent critiqué pour la véracité de ses articles, certains créant de toute pièce une information (création d'un personnage, d'une île, d'une bataille…) tandis que d'autres respectent les faits mais donnent leur point de vue sans nécessairement le signaler. Wikipédia qui se veut une encyclopédie collaborative mondiale apparait alors comme une source de désinformation, voire de manipulation. Des exercices sont ainsi réalisés dans les écoles et universités où l'on demande aux étudiants de repérer les faux passages de tel ou tel article édité sur Wikipedia. ■■■

Cette confrontation à la vérification de l'information touche aussi bien le citoyen lambda que le journaliste, voire même l'entreprise qui doit s'assurer que rien de faux n'est dit à son sujet. Les nombreux cas de fausse information ont conduit les administrateurs des sites d'information, mais également les cybernautes à se mobiliser car le péril est réel. Si un site est jugé peu fiable, son audience diminue parallèlement et un autre site le supplante. Sans pour autant exagérer, c'est également un danger pour l'outil Internet en tant que tel car il est clairement interconnecté avec nos vies privées et professionnelles, son affaiblissement par des scandales liés à sa capacité à propager rapidement de fausses rumeurs aboutirait à une réflexion collective sur la place de l'information et son partage, sans réelle solution.

C'est pourquoi de nombreux sites internet cherchent des parades pour éviter une fausse information : il peut être question d'une vérification pré-publication, d'une vérification post-publication, avec un coût important pour le site si ce sont ses salariés qui doivent vérifier l'information. C'est ainsi que les sites misent désormais sur la mobilisation des internautes qui, de par leur nombre, peuvent rapidement repérer la fausse information. Cela peut se faire en commentant le faux article, en le signalant à un modérateur ou en avertissant sur le forum du site les autres utilisateurs jusqu'au retrait du dit article. Wikipedia a ainsi mis en place un système de modérateur et de signaux permettant au cybernaute de savoir si l'article a été vérifié, s'il manque des sources ou s'il est suspect, en raison de trop nombreuses modifications issues d'un panel de participants restreint.

Vérifier est fastidieux... mais pas impossible !

Le problème est plus compliqué lorsqu'il est question de vidéos et d'images surtout, car pour prouver que l'image est fausse, il fallait jusqu'à présent que l'auteur du cliché original se manifeste, qu'un cybernaute retrouve le fichier brut sur un autre site ou qu'un spécialiste de la photo analyse la photo et y repère des incohérences. Le temps nécessaire à chaque vérification étant trop long, surtout si l'on pense aux milliers de photos qui sont quotidiennement mis en ligne, que les grands médias (la BBC a été la première) ont acheté des logiciels capables de repérer toutes les modifications opérées sur une photo. Le risque de publier une fausse information/photo est donc considérablement réduit, mais pas inexistant, le contexte de la prise de la photo pouvant être modifié.

Ce tableau assez sombre de la valeur de l'information en fin de compte ne doit pas écarter l'idée qu'Internet s'autorégule par ses propres outils. Par exemple, l'achat de followers sur Twitter ou d'amis sur Facebook fausse l'intérêt que représente le cybernaute acheteur sur la Toile. Le candidat Romney pour l'élection présidentielle de 2012 s'est ainsi fait prendre à ce piège, car ces faux virtuels que l'on s'ajoute sur son compte n'ont de réel que leurs identifiants. Les faux amis et followers disparaissent soit par action de Twitter et Facebook, qui y jouent leur crédibilité, soit par le cybernaute acheteur lui-même qui demeure suspect avec ces avatars qu'il ne connait pas, qui écrivent des phrases sans sens et dans une langue étrangère de l'acheteur…

Il y a ainsi une forte communauté sur Internet qui vérifie les informations et qui de cette façon renforce l'intérêt et la valeur des sites inspectés. Mais ce qui est très intéressant et qui s'est particulièrement vu lors des dernières élections présidentielles américaines, c'est ce phénomène de « fact cheking ». Lorsqu'un homme politique parle à la télévision ou accorde une interview à un journal, ses dires sont le jour même confrontés à un examen souvent réalisé sur Internet, où à l'aide de graphiques, d'extraits d'articles, on peut démontrer que l'homme politique ne connait pas ses dossiers ou qu'il dit le contraire d'une déclaration passée. Cet exercice, stimulant intellectuellement, ne doit pas être sur apprécié : le journaliste ou la

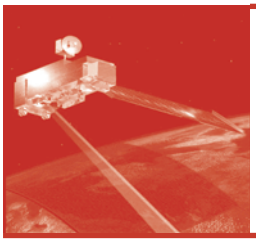
■■■ communauté d'internautes qui vérifient l'information peuvent se tromper (ils peuvent manquer de données connues des seuls protagonistes de l'affaire), mais surtout, l'auditoire qui suit la transmission télévisée n'est pas nécessairement identique à celui qui consulte les informations/vérifications en ligne. Il s'agit donc d'un travail salutaire mais imparfait et incomplet.

La vérification : un enjeu de pouvoir ?

Toutefois, il convient de rappeler que ce problème de la vérification de l'information n'est pas spécifique à Internet. Le plagiat de romans, de thèses de doctorat, les erreurs factuelles dans tel ou tel essai, en dépit de multiples relectures, rappellent que l'information est un enjeu de pouvoir qui doit être constamment surveillé pour ne pas être utilisé à mauvais escient. Néanmoins, il faut reconnaître qu'Internet, en faisant du cybernaute un potentiel acteur et créateur de l'information (les médias encouragent cette pratique qui leur permet d'être quasiment omniscients), brise les barrières traditionnelles du contrôle de l'information et favorise implicitement l'émergence de rumeurs et autres contrevérités.

L'optimisme doit cependant prévaloir, car même s'il y aura toujours de fausses informations qui circulent sur Internet, la mise en lumière de leur existence par des technologies de pointe, par les cybernautes, et leur correction ou leur suppression témoignent d'une vitalité intellectuelle certaine et d'une volonté de faire d'Internet un espace d'échanges d'informations et non de rumeurs. ■

*
* * *
*



La contagion du faux sur Internet

par François-Bernard Huyghe,
Directeur de recherche à l'IRIS

S'il est un thème qui revient systématiquement dans tout débat sur Internet, c'est bien celui du faux : le cyberespace est, par excellence, le lieu où chacun craint d'être trompé. L'utilisateur s'inquiète de ce qui se passe de l'autre côté de l'écran dans ce monde dématérialisé qu'il ne peut ni contrôler, ni vraiment comprendre. De plus, chaque internaute a fait l'objet d'au moins une tentative fut-elle aussi grotesque que celle de l'escroc, qui commence par vous appâter en vous proposant de faire transiter moyennant pourcentage quelques millions de dollars par votre compte.

Certes, il est possible d'écrire des livres mensongers sous-pseudonyme, de truquer des photographies ou de manipuler des images filmées. Et cela s'est vu ! Mais l'avénement du numérique a posé la question de la falsification en termes nouveaux.

La structure même du réseau au coeur de la question de l'authenticité

La structure même du réseau renvoie au problème de l'authenticité. Si vous voulez utiliser le réseau, il vous faut une interface matérielle (un ordinateur, un smartphone, une tablette...) et son équivalent sémantique – un nom d'utilisateur qui est enregistré par un fournisseur d'accès ou un réseau -, bref, une inscription. Or, chacun de ces dispositifs qui s'interpose entre votre identité physique et votre identité en ligne peut donner lieu à tromperie. Si les appareils sont identifiables (par exemple par une adresse IP), il n'est pas facile de prouver après coup qui se tenait physiquement derrière l'écran, surtout dans un cybercafé. Quant à l'identité déclarée auprès d'un fournisseur d'accès ou pour s'inscrire sur une plateforme, il va de soi qu'elle peut-être fausse.
Sans même parler du cas où le compte (ou le message, ou la transaction) n'émane pas d'une personne physique mais d'un robot, d'un algorithme qui parcourt le réseau pour y intervenir comme un humain. Cela ne signifie pas que n'importe qui puisse faire n'importe quoi anonymement sur la Toile : il existe des dispositifs d'enregistrement, de géolocalisation, d'identification, de traçage, etc. Même si tout le monde éprouve un sentiment d'impunité à agir derrière un pseudo ou un avatar ceux qui ont émis des Tweets racistes ou pratiqué la piraterie informatique peuvent parfois voir la police débarquer chez eux, éventuellement après une enquête relativement longue et coûteuse. Cela signifie simplement qu'il faut des connaissances techniques ou des protections politiques (comme un pays qui abrite des activités de piraterie sur son territoire) pour pratiquer des mystifications ou opérations illégales.

Le second domaine où s'introduit la possibilité du faux est celui du contenu même et ceci est inhérent au numérique qui autorise la reproduction parfaite, la combinaison parfaite et la modification indécelable du texte du son et de l'image. Le tout au bit ou au pixel près. Et comme de surcroît, la Toile met à notre disposition un nombre incalculable de documents ou de logiciels, même avec un talent très moyen, un utilisateur peut produire des textes pastichés, des photos retouchées, de faux sites ou des séquences vidéo remontées pour en détourner le sens. Ceci vaut qu'il s'agisse de « pomper » un mémoire universitaire, de pratiquer l'activisme politique, de faire une simple farce ou de monter une escroquerie.

À un troisième niveau, celui des systèmes, toute action offensive présuppose une forme quelconque de falsification. Dans la plupart des cas, cela équivaut à une usurpation d'identité : s'emparer d'un mot de passe, donner à un cerveau électronique des instructions illicites, qu'il s'agisse d'y prélever des données, de détraquer le fonctionnement de l'ensemble ou de le détourner à son profit. Qu'il y ait un défaut dans le système de défense, par exemple un mot de passe trop faible, ou qu'un humain ait été trompé, il n'y a pas de piraterie informatique sans une forme quelconque de tromperie envers un homme ou un logiciel. Cela revient, au final, à se faire passer pour quelqu'un d'autre, comme si l'on faisait croire à la machine que l'on est le propriétaire légitime.

La possibilité que les acteurs ne soient pas ce qu'ils prétendent, que les messages ne reflètent ni la réalité, ni l'intention de leur auteur, ou encore que les dispositifs de contrôle, abusés, ne fonctionnent pas comme ils devraient, tout cela hante le cybermonde. Et comme nous sommes de plus en plus dépendants – psychologiquement, culturellement, économiquement, politiquement – de systèmes de messagerie, gestion et transaction à distance, l'obsession de la tromperie empire.

La lutte de l'épée et du bouclier

Mais ce danger, que personne ne songe à nier, a suscité des contre-mesures. Certaines recourrent à la répression ou à la surveillance les plus classiques, comme l'obligation faire aux internautes chinois de donner leur véritable nom pour accéder aux blogs ou aux réseaux sociaux. D'autres sont des techniques de plus en plus sophistiquées de vérification et d'accréditation destinées à rendre des identités infalsifiables ou des protections sémantiques insurmontables. Elles nourrissent du reste une véritable industrie et ont lancé une classique compétition de l'épée et du bouclier avec les techniques de tromperie et de simulation. Mais la réponse pourrait aussi être culturelle : des attitudes de défiance systématique se développent et avec elles des pratiques comme le « fact checking » par les médias, c'est-à-dire l'examen systématique de tous les éléments qui, par exemple, devant des images sensées provenir d'une zone de combats, peuvent certifier la date, la localisation ou l'authenticité de ce que l'on voit. Sur les réseaux sociaux, les enquêteurs spontanés se multiplient, partant en quête de la documentation qui montrerait une tentative de tromperie et avertissant les autres. Celui qui se donne la peine d'aller chercher des éléments accréditant ou démentant une version de la réalité peut le faire ; il peut tout aussi bien se renseigner sur l'état de l'art en matière de trucage ou de piraterie.

Quitte parfois à tomber dans le défaut inverse, à douter de tout, on finit souvent par adopter les pires théories de la conspiration (une minorité cachée manipule tout, à commencer par les médias, on nous ment en permanence, tout est mis en scène, rien n'est vrai sauf le discours qui dit que rien n'est vrai...).

Nous retombons ici encore sur la question de la structure même des réseaux : ils se prêtent par nature à la diffusion rapide de thèses qui n'ont été accréditées par aucune source officielle ou professionnelle. Comme tout repose souvent sur la confiance que l'on accorde à son « semblable », présumé de bonne foi : le membre de sa « communauté », la nouvelle douteuse passe très vite de l'un à l'autre sur un modèle contagieux. Mais la vérité – ou au moins la volonté de vérifier et d'aller aux sources primaires – devient tout aussi contagieuse.

Tous ces éléments se contredisent et peuvent se résumer en un paradoxe – plus il y a de techniques de la communication, moins il y a de certitudes ; moins il y a de certitudes, plus on vérifie et on lutte contre la manipulation. Mais ce n'est pas en tombant dans la paranoïa ou en négligeant les conditions pratiques du phénomène que nous résoudrons ce paradoxe.

Rumeur et désinformation

La **rumeur** est souvent présentée comme « le plus vieux média du monde » puisque le bouche-à-oreille, le cancan, le potin, le commérage, le bruit, souvent la médisance sont sans doute nés avec le langage articulé. Pour définir plus précisément la rumeur, nous pouvons ajouter :

- qu'elle doit porter sur l'énoncé d'un fait
- qu'elle est toujours censée révéler quelque chose qu¹ignorait l'interlocuteur
- qu'elle suppose un incessant passage de l'information
- qu'elle n'est pas nécessairement mensongère ou erronée.
- qu'elle se caractérise par sa source présumée
- qu'elle peut être lancée délibérément
- que si l'intention perverse ne fait pas obligatoirement partie de la définition de la rumeur, on aurait beaucoup de mal à citer des rumeurs élogieuses.
- que, de la même façon, si la rumeur peut théoriquement porter sur tout, elle tend souvent à revenir sur les mêmes thèmes
- que, souvent, la rumeur fournit une explication d'apparence rationnelle donc rassurante à des faits dus au hasard
- que les nouvelles technologies ne freinent pas l'extension des rumeurs, au contraire.

La **désinformation** consiste, quant à elle, à propager délibérément des informations fausses pour influencer une opinion et affaiblir un adversaire. Le mensonge ici porte sur la réalité qu'il décrit (un fait imaginaire), sur la personne ou l'appartenance de qui la rapporte et, enfin, sur le but de son énonciation qui est de produire un dommage et non d'informer. Cela en fait une sorte de mensonge au cube. Cette stratégie agit indirectement contre quelqu'un et par un intermédiaire (médias, opinion abusée), d'où un jeu à trois -initiateur, public, victime qui peut faire appel à de véritables mises en scène ou à la construction d'une pseudo-réalité. La désinformation est souvent une version politique de la diffamation au sens pénal : le fait d'attribuer faussement à quelqu'un un comportement honteux. Le plus souvent, la désinformation impute à ses victimes de noirs complots, le plus habile étant parfois d'accuser la victime d'être elle-même désinformatrice et de décrédibiliser par avance tout ce qu'elle dira. Plus simplement, la désinformation accroît la confusion et le désordre. Elle est le contraire de ce que devrait être l'information au sens étymologique : in-formation, mise en forme. Paradoxe : Internet, en permettant à chacun de devenir éditeur presque sans contrôle et anonymement, a largement favorisé l'éclosion de la désinformation, notamment dans un cadre de guerre économique.

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques
2 bis, rue Mercoeur
75011 Paris - France
iris@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Secrétariat de rédaction : Pierre-Yves Castagnac